

PAS-PALVELUN PALVELUSOPIMUKSEN TURVALLISUUSLIITE SUOJAUSTASOLLE IV

SISÄLLYS

1	TURVALLISUUSLIITTEEN TARKOITUS	2
2	OSAPUOLET	2
3	VAATIMUKSEN MUKAISUUS	2
4	SALASSAPITO	2
5	POIKKEAMAT JA NIISTÄ VIESTINTÄ	3
6	TARKASTUKSET JA AUDITOINNIT	3
7	SUOJAAMISEN KEHITTÄMINEN	3
8	SOPIMUSKAPPALEET	3

1 TURVALLISUUSLIITTEEN TARKOITUS

Tämä asiakirja, *Turvallisuusliite*, on liite numero 6 [valitaan toinen: *Kulttuuriperintö-PAS*-palvelun palvelusopimukseen tai Fairdata PAS-palvelun palvelusopimukseen] (myöhemmin Sopimus). Tässä Turvallisuusliitteessä määritellään sopimuksen osapuolten velvollisuudet ja oikeudet sopimuksen kohteena olevaan palveluun hyväksytysti siirretyn aineiston (myöhemmin Aineisto) suojaamiseen liittyen.

Turvallisuusliite määrittelee periaatteet, joiden mukaisesti Osapuolet sitoutuvat noudattamaan hyviä turvallisuuskäytäntöjä, hyvää tiedonhallintotapaa sekä noudattamaan soveltuvaa lainsäädäntöä ja muita viranomaismääräyksiä palveluun siirrettyyn Aineistoon liittyen.

2 OSAPUOLET

Tämän turvallisuusliitteen osapuolet ovat Sopimuksen mukaisesti:

[Kopioidaan tähän Sopimuksen kohdasta "palvelusopimuksen osapuolet", jossa osapuolet "CSC" ja "hyödyntävä organisaatio"]

3 VAATIMUKSENMUKAISUUS

Sopimuksen kohteena olevan aineiston turvallisuusjärjestelyt toteutetaan alla mainittujen vaatimusten ja ohjeiden mukaisesti sopimuksen kattaman palvelun ja yhteistyön osalta:

1. Hyvä tiedonhallintapa
2. Tietoturvallisuuden hallintajärjestelmä vastaa ISO/IEC 27001:2013 standardin vaatimuksiin. Vastaavuus osoitetaan ulkopuolisella auditoinnilla.
3. Laki viranomaisen toiminnan julkisuudesta (621/1999): Lain 18 § 1 momentissa säädetään viranomaisen velvollisuudesta huolehtia siitä, että julkinen tieto on oikeaan aikaan käytettävissä ja velvollisuudesta suojata salassa pidettävät tiedot väärinkäytöltä.
4. VN asetus Tietoturvallisuudesta (681/2010) jossa säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista.

4 SALASSAPITO

Palvelun toimittaja sitoutuu

1. huolehtimaan Aineistosta suojaustason IV edellyttämän perustason tietoturvallisuusvaatimusten mukaisesti.
2. ettei Aineistoa käytetä hyväksi tai hyödyntää muuhun tarkoitukseen eikä luovuteta kolmannelle osapuolelle, ilman hyödyntävän organisaation lupaa.
3. että Aineistoa käsitellään yksinomaan säilyttämiseen liittyen välttämättömien toimenpiteiden yhteydessä ja että tarpeettomat aineistosta tehdyt kopiot hävitetään huolellisesti.
4. että Aineistoa ei siirretä ilman hyödyntävän organisaation nimenomaista lupaa maan rajojen ulkopuolelle.

5. että sekä onnistuneet että epäonnistuneet sisään kirjautumiset järjestelmään kirjoitetaan lokiin niin, että yksittäisen käyttäjän kirjautumiset järjestelmään voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti. Lisäksi huonolaatuisten salasanojen käyttö estetään.
6. ylläpitämään aineiston saantiin liittyvistä toimenpiteistä lokia, josta voidaan selvittää mitä Aineistoa on noudettu palvelusta, kenen toimesta ja milloin. Tämä kirjanpito tulee voida toimittaa hyödyntävälle organisaatiolle perustellusta pyynnöstä käyttökelpoisessa muodossa.
7. että toteutettavaksi valitut tietoturvatoinenpiteet ja -prosessit on organisoitu ja vastuutettu. Tietoturvallisuuden avainroolit on tunnistettu ja niille on nimetty varahenkilö tai -henkilöt.

Hyödyntävä organisaatio sitoutuu

1. ylläpitämään Aineistojen suojaustasoluokituksia sekä tiedottamaan palvelun toimittajalle näissä tapahtuneista muutoksista.
2. varmistamaan, että Palvelun käyttöön liittyviä tunnuksia säilytetään siten, ettei Palvelun käyttö ja Aineiston saanti ole oikeudettomasti tunnusten avulla mahdollista.

Salassapitovelvoite ei rajoita Osapuolten oikeutta hyödyntää tehtäviä suoritettaessa karttunutta yleistä ammattitaitoa ja kokemusta omassa toiminnassaan, kunhan salassa pidettävää tietoa ei paljasteta.

Osapuolet saattavat Aineistoon liittyvän salassapitovelvoitteen sopimuksen kattaman palvelun toimittamiseen tai ylläpitoon osallistuvan henkilöstönsä tietoon sekä sitoutuvat valvomaan ja vastaamaan, että se noudattaa tätä liitettä.

5 POIKKEAMAT JA NIISTÄ VIESTINTÄ

Jos Osapuoli havaitsee poikkeamia palveluun siirrettyjen aineistojen suojaamisessa tai salassapidossa, tulee Osapuolen ilmoittaa toiselle Osapuolelle havainnoistaan viipymättä. Tällaiset ilmoitukset välitetään Sopimuksen yhteys henkilöiden kautta. Poikkeamiin liittyvä viestintä toteutetaan yhteistyössä.

6 TARKASTUKSET JA AUDITOINNIT

Hyödyntävällä organisaatiolla on oikeus salassapidon puitteissa omalla kustannuksellaan tarkastaa etukäteen ilmoitettuna ajankohtana palvelun toimittajan turvallisuusjärjestelyt sopimuksen kohteena olevien Aineistojen osalta. Tarkastuksessa tulee käyttää ulkopuolista, molempien osapuolten hyväksymää auditoijaa, jonka tulee allekirjoittaa salassapitositoumus.

7 SUOJAAMISEN KEHITTÄMINEN

Osapuolet käsittelevät ja kehittävät yhteistyössä aineistojen suojaamista. Kehittämisessä huomioidaan molempien osapuolien vastuut aineistojen suojaamisessa. Merkittävät kehityskohteet käsitellään Sopimuksen muutostenhallinnan mukaisesti.

8 SOPIMUSKAPPALEET

Tätä liitettä on tehty kaksi (2) samansanaista kappaletta, yksi kummallekin osapuolelle.

_____, ____ / ____ 2019

Espoossa, ____ / ____ 2019

[hyödyntävä organisaatio]

CSC – Tieteen tietotekniikan keskus Oy

[nimi]
[nimike]

Kimmo Koski
Toimitusjohtaja